Prilex: POS malware evolves to target chip and PIN-protected cards

Kaspersky ⋮ 3-4 minutes ⋮ 5/26/2021

Kaspersky Lab researchers have revealed that the group behind the Prilex point-of-sale malware can now turn stolen credit card data into functional plastic cards. The evolved threat, which currently operates in Latin America is notable for its supportive, user-friendly business model that makes it worrying easy for attackers to launch attacks.

The use of 'smart' chip and PIN protected payment cards has spread globally over the last decade, and its growing adoption has inevitably attracted the attention of cyber criminals. Kaspersky Lab researchers monitoring financial cybercrime in Latin America have found that the Prilex malware has evolved to target this technology.

The Prilex malware has been active since 2014, and researchers have seen it migrate its efforts from ATM hacks to attacks on POS systems developed by Brazilian vendors, and now to using used stolen credit card information to create functional plastic cards. These allow a criminal to perform fraudulent transactions in any store, whether online or offline. This is the first time that the researchers have seen in the wild such a full suite of tools for carrying out fraud. The cloned credit card works in any point-of-sale system in Brazil due to a faulty implementation of the EMV standard that means not all data is verified during the approval process.

From a technical perspective, the Prilex malware comprises three components: malware that modifies the POS system and intercepts the credit card information; a server used to manage the illegally obtained information; and a user application that the malware 'client' can use to view, clone or save statistics related to the cards (such as how much has been stolen using that card). This is the most notable feature of the malware: its associated business model, where all the users' needs are taken into account, including the need for a simple and friendly user interface.

The evidence suggests the malware is distributed through the traditional postal service, convincing victims to grant computer access to the criminals for a remote support session, which is then used to install the malware. Most victims observed to date tend to be traditional shops, such as gas stations, supermarkets and typical retail markets; all located in Brazil.

"We are dealing here with a completely new malware, one that offers attackers everything from a graphic user interface to well-designed modules that can be used to create different credit card structures. Chip and PIN technology is still relatively new in some parts of the world, such as the U.S., and people may lack awareness of the risk of credit card cloning and abuse. In Brazil, the evolved Prilex malware takes advantage of a faulty implementation of the industry standards – highlighting the importance of developing secure, future proof standards for payment technologies," said Thiago Marques, security analyst at Kaspersky Lab.

For further information, please see the blogpost on Securelist.

Prilex: POS malware evolves to target chip and PIN-protected cards

Kaspersky Lab researchers have revealed that the group behind the Prilex point-of-sale malware can now turn stolen credit card data into functional plastic cards.